



ACCOUNTING INFORMATION SYSTEMS

ACC2400

Name of tutor: Dr. Ross Bloore

Tutorial time: Tuesday 8am

Name of Authors and student IDs:

Poojitha Sivakumar 28805925

Will Richards 27026329

Zhong Ye Quan 29053471

Joanna Lim Jia-Yen 29359538

Table of Contents

Introduction	2
Section 1- Sources of Risk and Control Measures	3
Section 2- Human Dimension of Information	5
Section 3- Disclosure of Breaches	7
Section 4- Data Breach at Target	9
Conclusion	11
Bibliography	13

Introduction

Cybersecurity is the protection of computing instruments or resources against unauthorised actions contradictory to the objectives and goals of the owning organization, by agents such as malicious applications (Kott, 2014). According to a Frost & Sullivan report commissioned by Microsoft (2018), Australian businesses potentially stand to lose up to an astounding total of 29 billion Australian Dollars per year due to cybersecurity incidents. This figure has sowed discord in the information technology industry, showing us how cybersecurity issues are becoming increasingly controversial and the need to imminently resolve them.

The swift growth in the availability and utilisation of digital data has posed critical challenges to modern businesses. Data appropriated from customers is highly sensitive and confers competitive advantages to businesses. This makes company data a significantly valuable target to external entities and is among the fundamental reasons why data breaches occur. Hence, companies must have sufficient measures and protocols in place to properly safeguard their data. Companies worldwide are projected to invest to a tune of almost \$96 billion in 2018 for the security of their information systems (Gartner, 2017). However, Pierre Audoin Consultants Ltd (2015) contraindicate that data breaches are ultimately unavoidable even with extensive spending on cyber security.

Based on the 2013 Target data breach case presented by Dubé (2016), the gravity of the consequences of cyberattacks and data losses has been made clear to the public. A study by the Ponemon Institute (2015) posits that a cyberattack is resolved in approximately 46 days, with an average total cost of almost \$1 million. To conclude, the effective mitigation of cyber threats requires a solid and methodical approach that includes identifying weak points in business

processes, analysing the impact of cyber incidents and an achievable action plan for the avoidance and mitigation of cyber risks.

Section 1- Sources of Risk and Control Measures

Part A:

According to Dube and Bernier (2011), sources of risk of data breaches arise from 4 main parties: employees, organisational partners, hackers and technological components. To prevent this, corporate and government organisations spend exuberant amount of money on instituting safety measures to protect data in strongholds. Target was the leading retailer company in cybersecurity, with extensive layers of protection and thus were well protected from data intrusions. Despite these preventative measures, Target faced a major data breach in 2013 due to hackers cleverly utilising the risk posed by the other three parties.

The hackers targeted an organisational partner, HVAC firm. Through phishing emails, they managed to get an employee to share the access code to remotely access the Target systems. This allowed them to bypass all the security layers and place a malware in the point-of-sale network used by cash registers.

Unaware and due to lack of training to recognise harmful programs, employees continued to use the registers to record and store transactional details. This unintentional action allowed the malware to copy the data and thus contributed to the leak. On the other hand, Target's cybersecurity team failed to assess the threat properly despite multiple alerts from state-of-the-art security system, FireEye, and their own anti-virus programs. Their negligence played a pivotal role in enabling the data breach. Correct action would have resulted in identification and removal of malware software before any data was leaked.

The data was copied to a Target web server. The hackers cleverly moved the data from this server to three external servers during the company's peak time to avoid detection. This allowed them to copy the card details and later on personal detail of each customer. This increased the severity of the problem and enabled to go unnoticed for a long period of time.

The malware they used took advantage of the lapse in security during sever processing. Server processing requires the raw data to be stored in RAM where it is unprotected for milliseconds. Within this time, the malware copied the data. Rapid development in technology causes gaps in security which us manipulated by such harmful programs.

Part B:

Recently, concern for risk management has elevated, leading to higher pressure for organisations in regard to breaches (Richard, Frank, Miles and Lucy,2004). Target should use the COSO framework to prevent future data breaches. The initial step should establish a system with integrity and ethical value by increasing the focus on ethics that should be followed by employees. By increasing accountability of employees, there will be a larger pool of people monitoring for suspicious activities and will be able to minimise the extent of a data breach or even prevent a breach from happening (Robert,2007). This should be complemented with a regular, basic training to identify malware or suspicious programs and to report them to the cybersecurity team.

To combat the risk posed by partnering organisations, Target can limit the access they have. This can be achieved by segmentation of the system and only offer access to the required parts. This will limit the access hackers gain if they manage to obtain the firm's user code and

password. Furthermore, Target should request partner organisations to improve their cybersecurity before allowing remote access.

High vigilance for data breaches and malware by Target's and partner organisations' cybersecurity systems will significantly increase difficulty of hackers gaining access into the system and thus will demotivate them.

The terminals should be constantly upgraded to ensure that the data is never unprotected. This will prevent the possibility of data leaks. Additionally, the full extent of the security programs should be used. This will decrease risk contributed by human judgement (Tsukiyama, 2018).

Section 2- Human Dimension of Information

Data breaches are to a great extent attributable towards human behaviour. Howarth (2014) states that the human element is involved in 95 percent of all cyber security incidents. Both Parsons et al. (2017), and Mitnick & Simon (2002) further reiterate this by concurring that in the safeguarding of an organisation's information systems, humans are the most vulnerable element. Upon further analysis, this is due to the flexible and impressionable nature of the human mind, unlike machines which are rigid and can only perform programmed tasks.

The human aspect is involved at least twice in the Target data breach. Target made significant investments in improving their infrastructure's security, but access to their systems were improperly managed by system administrators. External contractors had more access than required, and they did not possess adequate training against phishing emails and other forms of social engineering. The employee who divulged system credentials had most probably done so

due to affective commitment, or the emotional satisfaction gained from “helping” an influential organisation which Workman (2007) also suggests.

The effects of the Target data breach could have been lessened much earlier. Due to human aspects, the repercussions of the breach were actually worsened. Security experts at Target had shut off security features due to their apprehension towards new technology, and also ignored warnings of highest-priority issued by the systems. This is because humans, by nature, are resistant to change. Humans view security policies and implementations as obstacles and hence, they tend to ignore or delay carrying out the appropriate security actions. (Pfleeger & Caputo, 2012). With a clouded judgement in security risk identification, humans will find it more challenging to contain security risks and to recognise the costs of their actions, as demonstrated by these experts.

Hence, human error caused by lapses in judgement caused Target’s IT department to have a myopic approach towards security, and this set up perfect conditions for the breach to occur. If not for human aspects, this breach would not have happened, as the initial social engineering attempts at acquiring Target’s system credentials would not have been successful. To summarise, Schneier (2000) further reinforces the influential part the human dimension plays in information security with a powerful quote: *“Only amateurs attack machines; professionals target people.”*

Section 3- Disclosure of Breaches

Part A:

Maximising profits remains as one of the key goals for organisations (Engelbrecht, 2017), hence companies may be quite hesitant to disclose their data breaches. However, there are legislations regarding when an organisation should disclose its breaches.

The Notifiable Data Breaches Scheme (NBD) poses an obligation to the organisations to “disclose the data breach to any individual whose personal information is involved” (OAIC, 2018). The Office of Australian Information commissioner (OAIC) sets out guidelines and procedures an organisation needs to follow when an “eligible data breach” has occurred. When the organisation has identified that there is a data breach with reasonable evidence then it is obligated to “promptly notify individuals at likely risk of serious harm” (OAIC, 2018). In addition, they need to send a statement to the Commissioner regarding their breach. The Commissioner also includes a checklist for what sort of information needs to be disclosed to individuals who are affected.

On the other hand, reputation is another affects the decision of the business to disclose. It is likely to lose customers’ trust, potentially affect their customer base and sales. When customers are notified of the breach, this will increase the level of chaos which disproportionate to the risk the breach poses. This in turn leads to “an unwarranted loss of confidence” (Gregory, 2012) within the organisation. Hence, disclosing the breach to those who are affected of the “eligible” breach is deleterious to the company’s reputation, which affects all the people of the organisation and not only those who are affected.

Part B:

It is necessary for any organisation to be transparent with its operations in order to maintain a trustworthy relationship with the customers. When an organisation hesitates to disclose data breach they are willingly or unwillingly posing a risk to all potential members who are affected by the breach. The company is blinding its customers when there are chances that “someone could be using [their information]” while “they wouldn’t even know yet” (Tsukiyama, 2018). Instead, an organisation should disclose the information as soon as they have identified it as an “eligible risk” (OAIC) so that people who are affected can take necessary actions to protect their information. When the company notifies those who are affected, this could potentially “rebuild public trust” (Tsukiyama, 2018), this would highlight to their customers that the company puts emphasis in issues related to security and privacy seriously, which aids the damage in the company’s reputation. In addition, disclosing the breach to the victims shows the “ethical stance of the organisation”, by informing the consumers and obliging the legislation the organisation could reduce the consequences posed from the breach.

Part C:

Despite being notified from a malware detection tool regarding potential fraud activity, until it was informed by the U.S. Department of Justice, Target did not take any action. After being informed it took Target 12 days to act and investigate it further. Once Target was able to determine that there was a breach, they released a public statement highlighting the breaches and informing to the public regarding how “serious” this issue is to them (A bullseye view, 2013). The duration Target took to disclose the breach, “hackers could have sold all the information” (Tsukiyama, 2018).

When they had multiple alerts in relation to the malicious activity, Target must have emphasised and given priority to investigating the issue. However, Target neglected the alerts hence highlights the importance they show for security and privacy. Hence, like suggested by Professor Woodrow Hartzog (2015), it should be mandatory for organisation to take preventative measures to avoid such circumstances. Although, there are law enforcements regarding safety of privacy, it is also the ethical protocol that an organisation is expected to undertake during its operations.

Section 4- Data Breach at Target

Equifax works to estimate and report credit risk of consumers. Retail banking organisations use Equifax to assess the suitability of customers for new loans. In September of 2017, Equifax officially notified the public that their systems, including their customer's data had been breached by unauthorised individuals. Whilst estimates vary about the extent of information accessed by the hackers, the Wall Street Journal has reported that as many 146 million customer files may have been accessed (Andriotis, 2018). In addition the Wall Street Journal has suggested that the hackers had access to the files for four months prior to Equifax detecting their presence in July.

There has been significant criticism levelled at Equifax for the way they have handled the breach. One key criticism is the lack of action on Equifax's behalf, when Cisco reported a security flaw in a system used by Equifax in March, the company failed to successfully introduce a patch. Upon detecting the breach in July, Equifax did act, however much of the information had already been accessed by hackers (Andriotis, Rapoport & McMillian, 2017). This slow reaction, in addition to the time taken to publicly disclose the breach has been the

cause of much concern for regulators, investors and consumers (Newman, 2017). However, since the information has become available to the public, Equifax has taken more significant action. It was reported that Equifax had begun complete reviews of their security systems with help of an external firm. In addition, they have publicly declared their willingness to work with legislators and external investigators. The company has also been going through a significant movement of executive staff, as reported by business insider (Logan, 2017). This suggests the company's willingness to start afresh and rebuild its reputation.

Whilst the company has not publicly disclosed the weaknesses in internal controls which may have contributed to the extent of the breach, there has been significant commentary on Equifax's failures. From a series of investigations by journalists and regulators, it is clear there were a number of shortfalls in Equifax's internal control processes. Firstly, a report completed by the United States Government Accountability Office (2018) examined an out of date digital certificate which compromised the ability of Equifax to detect unauthorised activity on their servers. This in turn extended the period of time hackers had on the server and allowed them to gather even greater amounts of information. This is a clear failure in Equifax's detection controls.

Equifax also failed in a number of their preventative controls, such as poor security on passwords and on segmentation of their systems to hopefully contain any breach. However, the flaw which was most directly linked to the breach was Equifax's inability to maintain up-to-date patches of their security systems. As mentioned previously, there had been reports of a flaw in the Apache Struts system which Equifax uses. Apache Struts gave clear instructions to update the system with a patch to protect against the flaw. However, Equifax failed to action maintenance of its systems until after they detected the hackers on their system. This a clear

and present failure of Equifax to maintain their preventative controls was directly responsible for their vulnerability. Whilst some may argue that even with the patch the hackers may have accessed the system, it is certain that the failures to regularly maintain the system heightened the risk of a breach.

Conclusion

The security of customer and business data is of the utmost important to modern organisations. Businesses which fail to prevent unauthorised access to their data will likely suffer tremendous external and internal consequences, as the Target case and this article highlight. Whilst investment in strong defence of intellectual resources such as customer data, is expensive and time consuming, the costs associated with the organisations image and public scrutiny can be significantly worse. In saying this, in the long run Target may reduce these costs by taking advantage of opportunities.

Firstly, the response of Target has been to invest heavily in technologies and programs which will protect consumer data and reimburse affected customers. Whilst their initial response to hide the breach from public knowledge, would negatively affect their image, their willingness to investigate and improve has been forthright and made public. For example, their intention to bring forward a chip-card and identification system will show strong intention of the company to ensure customer security. Secondly, the breach of Targets systems allowed the public and shareholders to identify poor management practices within the business and make the appropriate personnel and structural changes. It is preferable to identify these practices via mechanisms such as internal audit, that don't result in massive consequences for brand.

However, it is still a benefit to the relevant parties that the appropriate changes were identified and made, as to ensure Targets long term growth and survival.

Overall the case is a clear demonstration of the dangers presented by managing a significant amount of customer data. What the case highlights is that strong internal control practices are vital in protecting an organisation against external threats. The costs of implementing these mechanisms may be extensive, however the costs associated with a breach are far greater.

Bibliography

- A BullsEye View. (2013). Target Confirms Unauthorised Access to Payment Card Data in U.S. Stores. Retrieved from <https://corporate.target.com/press/releases/2013/12/target-confirms-unauthorized-access-to-payment-card> [Press Release]
- Andriotis, A. (2018). Equifax Hack Might Be Worse Than You Think. *The Wall Street Journal*. Retrieved from <https://www.wsj.com/articles> [News Article]
- Dubé, L. (2016, March). Autopsy of a Data Breach: The Target Case. *International Journal of Case Studies in Management*, 14(1). [Journal Article]
- Engelbrecht, G. (2017). Rebuilding trust. *Accountancy SA*, , 2. Retrieved from <https://search-proquest-com.ezproxy.lib.monash.edu.au/docview/1937371940?accountid=12528> [Journal Article]
- Gartner. (2017). Gartner Forecasts Worldwide Security Spending Will Reach \$96 Billion in 2018, Up 8 Percent from 2017. Ergham, United Kingdom. Retrieved from <https://www.gartner.com/newsroom/id/3836563> [Press Release]
- Greenwald, J. (2012). Data breaches evolve from nuisance to major business threat. *Business Insurance*, 46(12), 4-6. [Journal Article]
- Gregory, M.A. (2012). 'You've been hacked': why data-breach reporting should be mandatory. Retrieved from <https://theconversation.com/youve-been-hacked-why-data-breach-reporting-should-be-mandatory-10220> [News Article]

- Hartzog, W. (2015). Prepared Testimony and Statement for the Record. Retrieved from <https://docs.house.gov/meetings/IF/IF17/20150127/102842/HHRG-114-IF17-Wstate-HartzogW-20150127.pdf> [Journal Article]
- Howarth, F. (2014). *The Role of Human Error in Successful Security Attacks*. Retrieved from <https://securityintelligence.com/the-role-of-human-error-in-successful-security-attacks/> [Journal Article]
- Kott, A. (2014). Towards Fundamental Science of Cyber Security. In R. E. Pino (Ed.), *Network Science and Cybersecurity. Advances in Information Security* (Vol. 55, pp. 1-13). New York: Springer. doi:10.1007/978-1-4614-7597-2 [Book]
- Logan, B. (2017, September 6). 2 top Equifax executives are leaving after a massive hack that exposed 143 million Americans' financial data. *Business Insider*. Retrieved from <https://www.businessinsider.com.au> [News Article]
- Microsoft. (2018, June 26). Direct costs associated with cybersecurity incidents costs Australian businesses \$29 billion per annum. Sydney, Australia. Retrieved from <https://news.microsoft.com/en-au/features/direct-costs-associated-with-cybersecurity-incidents-costs-australian-businesses-29-billion-per-annum/> [Website Release]
- Mitnick, K. D., & Simon, W. L. (2002). *The Art of Deception: Controlling the Human Element of Security* (1st ed). Retrieved from <http://sbisc.ut.ac.ir/wp-content/uploads/2015/10/mitnick.pdf> [Book]

- Parsons, K., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Computers & Security*, 66, 40-51. Retrieved from <http://www.sciencedirect.com/science/article/pii/S0167404817300081> [Journal Article]
- Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security. *Computers & Security*, 31(4), 597-611. Retrieved from <http://www.sciencedirect.com/science/article/pii/S0167404811001659> [Journal Article]
- Pierre Audoin Consultants Ltd. (2015, June). *Is a cyber breach inevitable? Cyber Security Challenges in the Netherlands*. CGI. Retrieved from <https://automatie-pma.com/wp-content/uploads/2015/05/CGI-Cyber-Security-White-Paper-Final.pdf> [Whitepaper]
- Ponemon Institute. (2015). *2015 Cost of Cyber Crime Study: Global*. Retrieved from http://www.cnmeonline.com/myresources/hpe/docs/HPE_SIEM_Analyst_Report_-_2015_Cost_of_Cyber_Crime_Study_-_Global.pdf [Research Report]
- Robert.P.M(2007).COSO Enterprise Risk Management: Understanding the New Integrated ERM Framework. Retrieved from <https://trove.nla.gov.au/work/25766690> [Book]
- Schneier, B. (2000). Semantic attacks: the third wave of network. In *Crypto-gram newsletter*. Retrieved from <https://www.schneier.com/crypto-gram/archives/2000/1015.html#1> [Newsletter]

Tsukayama, H. (2017). Why it can take so long for companies to reveal their breaches.

Retrieved from https://www.washingtonpost.com/news/the-switch/wp/2017/09/08/why-it-can-take-so-long-for-companies-to-reveal-their-data-breaches/?noredirect=on&utm_term=.2e8010622393 [News Article]

United States Government Accountability Office (2018). *Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach* (GAO-18-559). Retrieved from <https://www.gao.gov/assets/700/694158.pdf> [Government Report]

Workman, M. (2007). Gaining Access with Social Engineering: An Empirical Study of the Threat. *Information Systems Security*, 16(6), 315-331. doi:10.1080/10658980701788165 [Journal Article]